UNITED STATES PATENT AND TRADEMARK OFFICE

mn

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/773,763	02/05/2004	Peter Sim	10824-016001	5572

20985 7590 08/03/2007
FISH & RICHARDSON, PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
08/03/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/773,763	**Applicant(s)** SIM, PETER	
	Examiner Farid Homayounmehr	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 March 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application, filed 2/5/2004; amendment filed 3/29/2007.

2. Claims 1-24 are pending in the case.

Response to Arguments

3. Objection to claim 21 is withdrawn due to amendments by the applicant.

4. With regards to rejection under section 112, 1st paragraph to claim 9, applicant states: "It is admitted that those having ordinary skill in the art certainly understand that one piece of hardware could be specialized for ATM, another specialized for SONET. This does not require optimization, and in fact the top of page 3 goes so far as to call this "trivial to a person skilled in encryption of data packet". Therefore, the applicant relies on what is known in the prior art to meet the disclosure requirement for using hardware specialized for ATM and hardware specialized for ATM. Accordingly, the rejection is hereby withdrawn.

Applicant argues the same with respect to 112, first paragraph of claim 10. Therefore, the applicant relies on what is known in the prior art to meet the disclosure requirement for using a security interlock with a memory erasure function. Accordingly, the rejection is hereby withdrawn.

5. With regards to rejection of claim 1 under section 102, applicant argues that the amendments to claim 1 are not taught by the reference Minear. The newly added limitations are discussed in the new grounds of rejection outlined in the next section. It is also noted that in page 12 of their response, applicant states: "However, Claim 1 is also amended to recite that the lower speed cryptosystem also carries out at least one function other than encryption and decryption." However, no such limitation was found in the claim at hand.

With regards to claim 2, applicant argues: "Even if the Microsoft document states that FPGAs are "commonly used to develop hardware modules", there is no disclosure that FPGAs have been commonly used to develop crypto modules that are configured to carry out a specific encryption or decryption operation." Applicant also states: "Nowhere is there any disclosure of this, or any suggestion of this, in the prior art". However, there are many instances in prior art that FPGAs are used to carryout specific encryption or decryption operations. For example see claim 34 of US Patent No. 6'907'126, to Inada, filed April 18, 2001, or Col. 19, lines 22-42 of US Patent No. 7'106'860, to Yu, filed Feb. 6, 2002.

With respect to claim 4, applicant argues that Minear does not teach the limitation of a key management subsystem that communicates using a network management and is separate from the processing part. However, Minear col. 5 lines 47-64 teaches establishment of a security association between Minear's systems based on IPSEC. Establishing security association requires a database to store keys. It is also noted that keys for communication must be stored in communicating parties, which are separate. Also, the parties exchange key data and other security association related data using a network management protocol. Therefore, all elements required by claim 4, is disclosed by Minear. In addition, development of security systems based on a distributed system architecture was well known in the art. Distributed system architecture teaches development of different parts and modules of a system in separate devices, connected via a network.

With respect to claim 11, applicant argues that the packet headers are required to be replaced or removed, but IPSEC only encapsulates the headers. However, IPSEC is in IP layer. As packets traverse through different layers of the IP communication model (i.e. physical, data link, network layers), each layer adds and strips the header associated with that layer. In addition, Low's figure 4 and associated text clearly teaches removing and adding cryptographic headers.

With respect to claim 13, applicant argues that SNMPV3 Is not suggested by Minear. However, as mentioned in rejection of claim 5, SNMPV3 is just a version of SNMP, which is well known for network management as identified by the Microsoft document.

Applicant's argument relative to claims 12-23 is substantially the same as their arguments discussed and addressed above.

With respect to claims 9 and 24, applicant argues that although Gai teaches applying this method to both ATM and SONET, it does not specifically teach specific cards , one specialized for ATM and one for SONET. However, as admitted by the applicant, card specialized for ATM and cards specialized for SONET were well known to the one skilled in the art. It would have been obvious to the one skilled in art to use a separate card for each protocol.

With regards to claim 10, applicant argues: "Applicants will freely admit that tamper protection circuitry is well-known in the art. However, there is no teaching, suggestion or disclosure of using tamper protection circuitry to protect cryptographic keys, either in this art or in any other art." However, use of tamper protection circuitry to protect cryptographic keys was suggested in the art prior to applicant's invention. As an example, see paragraph 5 of US Application Publication No. 2004/0102181, to Horn, filed Nov. 5, 2001.

Following is the detailed rejection of claims 1-24:

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1 to 8 and 11 to 23 rejected under 35 U.S.C. 103(a) as being unpatentable over Minear (US Patent No. 5,983,350, dated 11/9/1999), and further in view of Low (US Patent No. 6,959,346, filed 12/22/2000).

6.1. As per claim 1, Minear is directed to a network encryption system (Fig. 1 items 14 and 18 and associated text, e.g. column 3 line 60 to 65), comprising: a first network interface, adapted for connection to a protected network; a second network interface, adapted for connection to an unprotected network Fig. 1, where the Internet is the unprotected network and the workstations are protected networks, as described in column 3line 50 to 56 and also claim 6); a processing part, which manages the encryption of information payload to be sent to the unprotected network, and decryption of information payload which are received from the unprotected network Fig. 2 item 50 and column 5 line 65 to column 6 line 20), and said processing part includes a microprocessor therein (column 5 line 65 to 67 describes that the proxy processes messages, therefore it has a processor and microprocessors are commonly used to process information); and an encryption and decryption system, including a first high-speed crypto system which operates using dedicated hardware components for cryptographic encryption and decryption of a first format kind of message, a second high-speed crypto system physically separate from said first high-speed crypto system using dedicated hardware components for cryptographic encryption and decryption of a second format kind of message different than said first format kind of message, and a second, lower speed crypto system, which carries out said cryptographic operations without dedicated hardware components. Fig 4 items 82 and 84 and column 11 lines 53 to 63 teach a first high-speed crypto system which operates using dedicated hardware components for cryptographic encryption and decryption, and the second lower speed crypto system which carries out said cryptographic operations without dedicated hardware. Although Minear teaches a cryptographic system to encrypt and decrypt using dedicated hardware, it does not specifically teach the use of two physically separate high-speed crypto systems, to process messages with two different formats.

Low's Fig. 4 and 5 and their associated text teach a system including multiple processors, and buffers, where each packet will have a header inserted, which identifies which processor the packet should be sent for processing. The decision is based on the information inside the packet. Therefore, Low teaches a first high-speed crypto system which operates using dedicated hardware components for cryptographic encryption and decryption of a first format kind of message, a second high-speed crypto system physically separate from said first high-speed crypto system using dedicated hardware components for cryptographic encryption and decryption of a second format kind of message different than said first format kind of message.

Low and Minear are analogous art as they are both directed to a network system security using cryptographic techniques.

At the time of invention, it would have been obvious to the one skilled in art, to enhance Minear's system to include multiple processors, each capable of processing different cryptographic processes. The motivation to do so would have been to increase the system flexibility in accommodating different types of encryption protocols, as suggested by Low's col. 3 lines15-57.

6.2. As per claim 2, Minear is directed to a system as in claim 1, wherein said first high-speed crypto system uses field programmable gate arrays which are configured to carry out a specific encryption or decryption operation (field programmable gate arrays (FPGA) are commonly used to develop hardware modules, as per their definition in "Microsoft Computer Dictionary, ISBN: 0-7356-1495-4, copyright 2002". Also note that use of FPGAs to carryout specific encryption or decryption operations was well known in the art. For example see claim 34 of US Patent No. 6'907'126, to Inada, filed April 18, 2001, or Col. 19, lines 22-42 of US Patent No. 7'106'860, to Yu, filed Feb. 6, 2002).

6.3. As per claim 3, Minear is directed to a system as in claim 1, wherein said first low-speed crypto system includes a first portion using a cryptographic processor, and a second crypto portion using software running on a general-purpose processor (column

11 line 54 to 58 describes an interface between the software and Hardware module, which allows the software module to use the Hardware module).

6.4. As per claim 4, Minear is directed to a system as in claim 1, further comprising a key management subsystem (column 5 line 63 to 64), physically separate from said processing part (Minear col. 5 lines 47-64 teaches establishment of a security association between Minear's systems based on IPSEC. Establishing security association requires a database to store keys. It is also noted that keys for communication must be stored in communicating parties, which are separate. Also, the parties exchange key data and other security association related data using a network management protocol. In addition, development of security systems based on a distributed system architecture was well known in the art) and connected to said processing part via a network interface and communicating using a network management protocol, said key management subsystem storing encrypted software keys therein (column 7 line 22 to 37. Note that private keys are protected from public access.).

6.5. As per claim 5, Minear is directed to a system as in claim 4, wherein said key management subsystem and said processing part communicate via Simple Network Management Protocol (SNMP is commonly used to manage the communication between Hardware and Software modules, as per their definition in "Microsoft Computer Dictionary, ISBN: 0-7356-1495-4, copyright 2002". SNMPV3 is just a version of SNMP).

6.6. As per claim 6, Minear is directed to a system as in claim 4, wherein said key management subsystem stores at least one private key by encrypting said keys using a password for the encryption (per column 7 line 34 to 36, access to keys are allowed for administrators and key management daemons only. Administrators authenticate themselves using passwords. Therefore, their password is part of the encryption process).

6.7. As per claim 7, Minear is directed to a system as in claim 4, wherein said key management system maintains addresses of other key management systems (Minear uses IPSEC to setup secure connection between firewalls. As described in column 4 line 7 to 43, the keys used in encryption/decryption process are identified in Security Associations. The Security Associations are identified by destination address. The other key management system is at the destination. Therefore, the address of the other key management system is maintained.).

6.8. As per claim 8, Minear is directed to a system as in claim 1, wherein said first high-speed crypto system includes at least one card (column 12 line 23 to 26).

6.9. As per claim 11, Minear is directed to a system as in claim 1, wherein said encryption and decryption system includes a portion which removes a header associated with the network interface, replaces said header with a cryptographic header, processes said message using the cryptographic header, and then generates a new header associated with the network interface (as described in column 3 line 57 to column 4 line 28, Minear uses IPSEC protocol which includes the authentication header (AH) and encapsulated payload (ESP) methods. AH and ESP remove and replace the packet header with a protocol header at the sending side, process the packet using the protocol headers, and strip the protocol header and rebuild the original header at the destination side. For more information on AH and ESP, see IETF RFC 1825 to 1829. Also, Low Fig. 4 and 5 and associated text teaches adding and removing headers to identify the processor that processes the packet).

6.10. Claims 12 to 21 are substantially the same as claims 1 to 11.

6.11. As per claim 22, Minear is directed to a method comprising: connecting to a first network which is a protected network and a second network which is an unprotected network; encrypting data being sent from said first network to said second network, and decrypting data being sent from said second network to said first network (see response to claim 1); and storing and managing at least one signing key in a separate unit from the unit carrying out the encrypting, and communicating with said separate unit, over a separate network from said first and second network (column 10 line 30 to 52 describes Network separation to protect the network from being attacked by an attacker who has obtained the control of one network node. Protocol data, which includes keys, are transferred between separate elements, each of which is responsible for a particular functionality. The network separation ensures protection of data (e.g. keys) within one element from other elements).

6.12. As per claim 23, Minear is directed to a method as in claim 22, wherein said encrypting comprises removing a header associated with a network protocol of said second network; obtaining key information from said separate unit, and forming an encryption header based on said key information and associating said encryption header with a message fragment; encrypting the message fragment, using said encryption header; and regenerating the header associated with the network protocol (see the response to claim 11).

7. Claims 9, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Minear and Low as applied to claims 1 to 8, and 11 to 23 above, and further in view of Gai (US Patent Application Publication No. 2004/0160903 A1, dated 8/19/2004).

7.1. As per claim 9, Minear is directed to a system as in claim 8. Minear teaches a system for encryption of packets in a packet switched data network by describing the system using IPSEC as an example. Although Minear's system is not limited to IPSEC or Internet protocol and does work with other packet switching protocols, the disclosure does not specifically mention application of the system in ATM or SONET.

Gai is directed to a network security system which facilitates the process of packet encryption (paragraph 42) by applying security tags. Gai's disclosure specifically includes application of his method to ATM and SONET networks (paragraphs 102 and 103), as it teaches encryption/decryption performed in any network element that handles packet forwarding.

Minear and Gai are analogous art as they are both directed network security and packet encryption/decryption.

At the time of the invention, it would have been obvious to a person skilled in art to include the idea of packet encryption/decryption of ATM and SONET packets as taught by Gai, in the security system of Minear, to control the flow of messages.

The motivation to do so would have been to expand the applicability of Minear's message flow control system to include ATM and SONET systems.

Furthermore, if the network includes ATM and SONET packets, it would have been obvious to a person skilled in the art to use a separate card for each packet type (SONET or ATM) to process the encryption/decryption of packets for each packet type.

Gai also teaches use of his method in Ethernet and Fiber Channel networks (paragraph 98 to 100). Therefore, it teaches application of its systems in all layer 1, 2, and 3 protocols (paragraph 39), including Ethernet and Frame Relay (packet switching protocols in layers 1 and 2. Note also that, as mentioned in section titled Response to Arguments, use of specialized cards to perform cryptographic processings for different applications was well known in the art).

7.2. As per claim 24, Minear and Gai are directed to a system as in claim 1, wherein at least one of said network interfaces is an Ethernet network (see the response to claims 1 and 9).

8. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Minear and Low as applied to claim 4 above, and further in view of King (US Patent Application Publication No. 6,426,706, filed 11/19/1998).

8.1. As per claim 10, Minear is directed to a system as in claim 4. Minear does not specifically teach a security interlock on said key management subsystem, and a memory erase function which erases said memory when said security interlock is violated.

King is directed to a security interlock (column 3 line 54 to 59), which detects tampering. King also teaches a memory erasure function that erases memory upon receiving a violation warning (column 3 line 65 to column 4 line 5).

King and Minear are analogous art as they are both directed to security systems. At the time of invention, it would have been obvious to a person skilled in art to combine the tamper resistant feature described by King with the system of Minear.

The motivation to do so would have been to protect the keys and other important data from disclosure in the case of a tampering attack.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571 272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

Examiner

Art Unit: 2132

Gilberto Barron

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100